UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

Douglas Paul Delaney and Nancy Marie Delaney Plaintiffs, v. Beltrami County; City of Bloomington; City of Brainerd; Carlton County; Crow Wing County; City of Eden Prairie; City of Hancock; Hennepin County; Hire Right, a Delaware Corporation; Kanabec County; City of Minnetonka; City of Mound; Metropolitan Airport Commission; City of Rosemount; St. Louis County; City of St. Paul; Michael Campion, in his individual capacity as the Commissioner of the Department of Public Safety; Ramona Dohman, in her individual capacity as the Commissioner of the Department of Public Safety; John and Jane Does (1 - 150) acting in their individual capacity as supervisors, officers, deputies, staff, investigators, employees or agents of the other governmental agencies; Department of Public Safety Does (1-30) acting in their individual capacity as officers, supervisors, staff, employees, independent contractors or agents of the Minnesota Department of Public Safety; and Entity Does (1-30) including cities, counties, municipalities, and other entities sited in Minnesota, Defendants.	Civil File No. **COMPLAINT** **JURY TRIAL DEMANDED**

For Plaintiffs' Complaint, for which Plaintiffs demand trial by jury on all claims so triable, Plaintiff Douglas Paul Delaney ("Douglas") and Plaintiff Nancy Marie

Delaney ("Nancy") (collectively referred to as "Plainitffs") hereby state and allege as follows:

INTRODUCTION

This is a case to redress the abuse of power by numerous law-enforcement personnel and public employees who illegally obtained the Minnesota Department of Public Safety's system for maintaining the personal, private information of Minnesota citizens. Officers and employees from over fifteen different law-enforcement agencies and entities chose to violate federal law, Minnesota and federal policy and the constitutionally and statutorily protected privacy rights of Plaintiffs Douglas Delaney, a former police officer, and his wife, Nancy Delaney. Douglas had his private personal information obtained or used approximately eighty-three times without a purpose permitted by the DPPA. Nancy had her private personal information obtained or used approximately twelve times without a purpose permitted by the DPPA.

These personnel violated the federal Driver's Privacy Protection Act ("DPPA") and violated Plaintiffs' civil rights under 42 U.S.C. § 1983, by unlawfully accessing Plaintiffs' protected driver's license information without any legitimate purpose. More disturbing, these personnel, charged with protecting and serving the public, knowingly abused their position of trust simply to satisfy their shallow desires to peek behind the curtain into the private lives of the Plaintiffs, without their knowledge or consent, and without ever informing them of their activities. In fact, they carried on these searches surreptitiously and concealed them from Plaintiffs and, presumably, from their supervisors and others. Those charged with oversight of the system, including the

Commissioners, concealed this from Plaintiffs by failing to ever notify them of these intrusions and violations, and concealed the extent of the violations from the general public. The utter disregard for their privacy rights by law-enforcement personnel, public employees, and others caused Plaintiffs' emotional distress and a logical fear for their personal safety.

The State of Minnesota, itself, has found that at least 50% of all officers statewide are engaged in the use of this database for impermissible purposes, and therefore violating federal civil and criminal laws. Moreover, the access permitted to law-enforcement officers, public employees, and others is easily obtained and makes highly private information available, including health information and social security numbers. Plaintiffs have no control over the Defendants obtaining their personal information, and impermissible, and inappropriate obtaining has been deliberately concealed and conducted in a surreptitious fashion. These Defendants are the window-peepers of the electronic data age. Through lax policies and apathetic enforcement of the law, these officials and governmental units have caused direct damage to Plaintiffs, just as they have trampled upon the clear legislative protections of all citizens' right to feel secure in their privacy.

General Background of Law and Facts

1. This is an action for injunctive relief and money damages for injuries sustained when personnel from various entities in Minnesota illegally obtained Plaintiffs' private, personal and confidential driver's license information without a legitimate or permissible law-enforcement purpose or any other lawful purpose.

2. These law-enforcement personnel, public employees, and others viewed and obtained Douglas' private information approximately eighty-three times between 2003 and 2012.

3. These law-enforcement personnel, public employees, and others viewed and obtained Nancy's private information approximately twelve times between 2004 and 2012.

4. Attached to this Complaint as Exhibit A is a copy of an audit prepared by the Minnesota Department of Public Safety showing the obtainments of Douglas' driver's license information by name, not license plate number, with his driver's license number removed, and showing the "station," meaning the police department, sheriff's office, or other government entity through which the officer obtained his information.

5. Attached to this Complaint as Exhibit B is a copy of an audit prepared by the Minnesota Department of Public Safety showing the obtainments of Nancy's driver's license information by name, not license plate number, with her driver's license number removed, and showing the "station," meaning the police department, sheriff's office, or other government entity through which the officer obtained her information.

6. Without legitimate, permissible reasons, these individuals obtained Plaintiffs' private information from Department of Vehicle Services' ("DVS") database or Bureau of Criminal Apprehension ("BCA") database.

7. Upon information and belief, these individuals further impermissibly used or disclosed Plaintiffs' private information without a permissible purpose.

8. Each unauthorized, impermissible use, disclosure, or obtainment of their private information, made without a permissible purpose and while acting under color of state and federal law, violated Plaintiffs' federal civil rights and constituted behavior prohibited by the federal constitution, federal statute, Minnesota statute, common law, and agency and departmental regulations prohibiting some or all of the conduct engaged in by Defendants in this case.

9. Plaintiffs bring this action pursuant to 42 U.S.C. §§ 1983 and 1988, the Fourth and Fourteenth Amendments of the United States Constitution, 28 U.S.C. §§ 1331 and 1343(a)(3), the Driver's Privacy Protection Act ("DPPA") 18 U.S.C. § 2721 *et seq.*, and Minnesota common law invasion of privacy.

10. The aforementioned statutory and constitutional provisions confer original jurisdiction of this Court over this matter.

11. This Court has jurisdiction over Plaintiffs' state law claims pursuant to 28 U.S.C. § 1367.

12. The amount in controversy exceeds $75,000, excluding interests and costs.

The Parties

13. Douglas Paul Delaney is, and was at all times material herein, a citizen of the United States and a resident of the State of Minnesota.

14. Nancy Marie Delaney is, and was at all times material herein, a citizen of the United States and a resident of the State of Minnesota.

15. Defendant Beltrami County is a county in Minnesota, which can be sued under Minn. Stat. § 466.01 *et seq.*

16. Defendant Carlton County is a county in Minnesota, which can be sued under Minn. Stat. § 466.01 *et seq.*

17. Defendant Crow Wing County is a county in Minnesota, which can be sued under Minn. Stat. § 466.01 *et seq.*

18. Defendant Hennepin County is a county in Minnesota, which can be sued under Minn. Stat. § 466.01 *et seq.*

19. Defendant Kanabec County is a county in Minnesota, which can be sued under Minn. Stat. § 466.01 *et seq.*

20. Defendant St. Louis County is a county in Minnesota, which can be sued under Minn. Stat. § 466.01 *et seq.*

21. Defendant City of Bloomington is a home rule charter city in Minnesota, which can be sued under Minn. Stat. § 466.01 *et seq.*

22. Defendant City of Brainerd is a home rule charter city in Minnesota, which can be sued under Minn. Stat. § 466.01 *et seq.*

23. Defendant City of Eden Prairie is a statutory city in Minnesota, which can be sued under Minn. Stat. § 466.01 *et seq.*

24. Defendant City of Hancock is a statutory city in Minnesota, which can be sued under Minn. Stat. § 466.01 *et seq.*

25. Defendant City of Minnetonka is a home rule charter city in Minnesota, which can be sued under Minn. Stat. § 466.01 *et seq.*

26. Defendant City of Mound is a statutory city in Minnesota, which can be sued under Minn. Stat. § 466.01 *et seq.*

27. Defendant City of Rosemount is a statutory city in Minnesota, which can be sued under Minn. Stat. § 466.01 *et seq.*

28. Defendant City of St. Paul is a home rule charter city in Minnesota, which can be sued under Minn. Stat. § 466.01 *et seq.*

29. Defendant Metropolitan Airport Commission is a public corporation under Minn. Stat. § 473.603 *et seq.*, which can be sued under Minn. Stat. § 466.01, *et seq.*

30. Defendant Hire Right, Inc. is incorporated in Delaware with a Registered Office Address in St. Paul, Minnesota.

31. Defendants Entity Does (1-30) are various unknown municipalities as defined by Minn. Stat. § 466.01, subd. 1 that can be sued under Minn. Stat. § 466.01 *et seq*. or other statutes, and federal departments and agencies, which can be sued under 28 U.S.C. § 1346 or other statutes.

32. Plaintiffs will refer to the entities named in paragraphs 12 to 31 above, along with the Entity Does, collectively as the "Defendant Entities" or "Entity Defendants."

33. Defendants John and Jane Does (1-150), upon information and belief, were, at all times material herein, citizens of the United States and residents of the State of Minnesota, duly appointed and acting in their individual capacities as law-enforcement supervisors, officers or employees of the Defendant Entities or other federal, state, county or municipal entities in Minnesota.

34. Plaintiffs will refer to the individual Defendants (with the exception of the "Commissioner Defendants," "Department of Public Safety Defendants" and "Supervisor Defendants" defined below), including John and Jane Does, collectively as the "Individual Defendants" or "Defendant Individuals."

35. Plaintiffs will refer to the Defendants with supervisory authority over the Individual Defendants, including any John and Jane Does with such supervisory authority, collectively as the "Defendant Supervisors" or "Supervisor Defendants."

36. Defendant Michael Campion ("Campion"), upon information and belief, was, at all times material herein, a citizen of the United States and a resident of the State of Minnesota, duly appointed and acting in his individual capacity as the Commissioner of the Minnesota Department of Public Safety.

37. Defendant Mona Dohman ("Dohman"), upon information and belief, was, at all times material herein, a citizen, of the United States and a resident of the State of Minnesota, duly appointed and acting in her individual capacity as the Commissioner of the Minnesota Department of Public Safety.

38. Plaintiffs will refer to the Defendants Campion and Dohman collectively, as the "Commissioner Defendants" or "Defendant Commissioners."

39. Defendants DPS Does (1-30), upon information and belief, were, at all times material herein, citizens of the United States and residents of the State of Minnesota, duly appointed and acting their individual capacities as officers, supervisors, employees, staff, employees, independent contractors or agents of the Minnesota Department of Public Safety.

40. Plaintiffs will refer to officers, supervisors, employees, staff, employees, independent contractors or agents of the Minnesota Department of Public Safety who created, installed, monitored, regulated, coded, enforced, supervised, maintained, oversaw, updated, or otherwise worked on the DVS database or BCA database, each of which contained Douglas' and Nancy's private driver's license information (collectively or individually, "DPS Databases" as "Department of Public Safety Does" or "DPS Does.")

FACTUAL ALLEGATIONS

41. Douglas and Nancy live in Cloquet, Minnesota.

42. Douglas attended Hibbing Community College and Hibbing Technical Institute.

43. Douglas became involved in law-enforcement since 1986, when he took a position as a Deputy Sheriff in the state of Wyoming.

44. Douglas started as a officer for the Metropolitan Airport Commission in 1991.

45. Douglas was forced to retire from the force, due to an injury that occurred on the job, in 1999.

46. Douglas voiced his concerns about certain local government actions in a publication that he believes aroused some interest and perhaps antipathy on the part of local government officials, which accounts for a portion of the look ups here.

47. Douglas was divorced from his first wife in 1993.

48. Douglas' ex-wife is friends with several law-enforcement personnel in Brainerd, Minnesota.

49. Nancy is currently employed as an Office Manager for a construction company.

50. Nancy attended college in Anchorage, Alaska, where she attained an accounting degree.

51. Douglas started dating Nancy in 2003.

52. Douglas and Nancy married in 2004.

Law Enforcement Officers and Personnel from Entities Across Minnesota Viewed Plaintiffs' Private Information Outside the Scope of Any Investigation or Official Police Business

53. The Driver and Vehicle Services Division ("DVS") of the DPS maintains a database containing the motor vehicle records of Minnesota drivers. ("DVS Database").

54. The DVS Database contains "personal information" and "highly restricted personal information," as defined by 18 U.S.C. § 2725 ("Private Data"), including but not limited to names, dates of birth, driver's license numbers, addresses, driver's license photos, weights, heights, social security numbers, various health and disability information, and eye colors of Minnesota drivers, both current and former information dating back to the driver's first license issued in Minnesota.

55. The Minnesota Driver's License Application states: "you must provide your Social Security Number…"

56. According to the Minnesota Driver's License Application, "[i]f you don't provide the information requested, DPS cannot issue you a driver's permit, license, or identification card, and your existing driving privileges, may be affected."

57. As early as 2003, Individual Defendants began looking up Plaintiffs' Private Data on the DVS Database.

58. After the Individual Defendants looked up Plaintiffs' Private Data, they gained knowledge of the contents of the Private Data. In gaining such knowledge, the Individual Defendants obtained Plaintiffs' Private Data.

59. Exhibits A and B, incorporated herein, reflect excerpts of an audit provided by DPS showing each time Plaintiffs' Private Data was obtained or used by an Individual Defendant.

60. Each act of the Individual Defendants in obtaining Plaintiffs' Private Data also constituted a disclosure by the Commissioner Defendants, because any release or access of information, whether permitted or not, necessarily requires a disclosure; and the method of setting up the DVS Database and of providing constant access to it constituted a disclosure of Private Data under the DPPA.

61. Column "EsupportStationName" of Exhibit A and B, incorporated herein, reflect the department or entity which, upon information and belief, employed the Individual Defendant that obtained or used Plaintiffs' Private Data.

62. Column "EsupportPath" of Exhibit A and B, incorporated herein, reflect the type of Private Data that was obtained or used by the Individual Defendant.

63. Columns "AccessDay" and "AccessDate," of Exhibit A and B, incorporated herein, reflect the day of the week, date, and time when the Individual Defendant obtained or used Plaintiffs' Private Data.

64. DPS does not provide the name of the individual who obtained or used Plaintiffs' Private Data.

65. Each line of Exhibits A and B, incorporated herein, reflect the audit of each time Plaintiffs' information, upon information and belief, was obtained or used by an Individual Defendant without a purpose permitted by the DPPA.

66. Officers employed by, licensed by, or otherwise accessing through Beltrami County obtained Douglas' Private Data, as reflected in Exhibit A for purposes not permitted by the DPPA four times.

67. Defendant Beltrami County's obtainment and use of Plaintiff's personal information was not for any use in carrying out any law enforcement, governmental, judicial, or litigation-related function.

68. Douglas has never been charged with or suspected of committing a crime in Beltrami County, has never been involved in any civil, criminal, administrative, or arbitral proceeding in or involving Beltrami County, and there was no legitimate reason for Plaintiff to have been the subject of any investigation by Beltrami County.

69. Rather, Beltrami County's obtainment and use of Plaintiff's personal information was for purposes that were purely personal to Beltrami County's personnel.

70. Officers employed by, licensed by, or otherwise accessing through the City of Bloomington obtained Douglas' Private Data, as reflected in Exhibit A for purposes not permitted by the DPPA two times.

71. Defendant Bloomington's obtainment and use of Plaintiff's personal information was not for any use in carrying out any law enforcement, governmental, judicial, or litigation-related function.

72. Douglas has never been charged with or suspected of committing a crime in the City of Bloomington, has never been involved in any civil, criminal, administrative, or arbitral proceeding in or involving the City of Bloomington, and there was no legitimate reason for Plaintiff to have been the subject of any investigation by the City of Bloomington.

73. Rather, the City of Bloomington's obtainment and use of Plaintiff's personal information was for purposes that were purely personal to the City of Bloomington's personnel.

74. Officers employed by, licensed by, or otherwise accessing through the City of Brainerd obtained Douglas' Private Data, as reflected in Exhibit A for purposes not permitted by the DPPA three times.

75. Defendant Brainerd's obtainment and use of Plaintiff's personal information was not for any use in carrying out any law enforcement, governmental, judicial, or litigation-related function.

76. Douglas has never been charged with or suspected of committing a crime in the City of Brainerd, has never been involved in any civil, criminal, administrative, or

arbitral proceeding in or involving the City of Brainerd, and there was no legitimate reason for Plaintiff to have been the subject of any investigation by the City of Brainerd.

77. Rather, the City of Brainerd's obtainment and use of Plaintiff's personal information was for purposes that were purely personal to the City of Brainerd's personnel.

78. Officers or personnel employed by, licensed by, or otherwise accessing through Carlton County obtained Douglas' Private Data, as reflected in Exhibit A for purposes not permitted by the DPPA ten (10) times.

79. Defendant Carlton County's obtainment and use of Plaintiff's personal information was not for any use in carrying out any law enforcement, governmental, judicial, or litigation-related function.

80. Douglas has never been charged with or suspected of committing a crime in Carlton County, has never been involved in any civil, criminal, administrative, or arbitral proceeding in or involving Carlton County, and there was no legitimate reason for Plaintiff to have been the subject of any investigation by Carlton County.

81. Rather, Carlton County's obtainment and use of Plaintiff's personal information was for purposes that were purely personal to Carlton County's personnel.

82. Officers employed by, licensed by, or otherwise accessing through Crow Wing County obtained Douglas' Private Data, as reflected in Exhibit A for purposes not permitted by the DPPA seven times.

83. Defendant Crow Wing County's obtainment and use of Plaintiff's personal information was not for any use in carrying out any law enforcement, governmental, judicial, or litigation-related function.

84. Douglas has never been charged with or suspected of committing a crime in Crow Wing County, has never been involved in any civil, criminal, administrative, or arbitral proceeding in or involving Crow Wing County, and there was no legitimate reason for Plaintiff to have been the subject of any investigation by Crow Wing County.

85. Rather, Crow Wing County's obtainment and use of Plaintiff's personal information was for purposes that were purely personal to Crow Wing County's personnel.

86. Officers employed by, licensed by, or otherwise accessing through the City of Eden Prairie obtained Douglas' Private Data, as reflected in Exhibit A for purposes not permitted by the DPPA two times.

87. Defendant Eden Prairie's obtainment and use of Plaintiff's personal information was not for any use in carrying out any law enforcement, governmental, judicial, or litigation-related function.

88. Douglas has never been charged with or suspected of committing a crime in the City of Eden Prairie, has never been involved in any civil, criminal, administrative, or arbitral proceeding in or involving the City of Eden Prairie, and there was no legitimate reason for Plaintiff to have been the subject of any investigation by the City of Eden Prairie.

89. Rather, the City of Eden Prairie's obtainment and use of Plaintiff's personal information was for purposes that were purely personal to the City of Eden Prairie's personnel.

90. Officers employed by, licensed by, or otherwise accessing through the City of Hancock obtained Douglas' Private Data, as reflected in Exhibit A for purposes not permitted by the DPPA three times.

91. Defendant Hancock's obtainment and use of Plaintiff's personal information was not for any use in carrying out any law enforcement, governmental, judicial, or litigation-related function.

92. Douglas has never been charged with or suspected of committing a crime in the City of Hancock, has never been involved in any civil, criminal, administrative, or arbitral proceeding in or involving the City of Hancock, and there was no legitimate reason for Plaintiff to have been the subject of any investigation by the City of Hancock.

93. Rather, the City of Hancock's obtainment and use of Plaintiff's personal information was for purposes that were purely personal to the City of Hancock's personnel.

94. Officers or personnel employed by, licensed by, or otherwise accessing through Hennepin County Economic Assistance obtained Douglas' Private Data, as reflected in Exhibit A for purposes not permitted by the DPPA one time.

95. Defendant Hennepin County's obtainment and use of Plaintiff's personal information was not for any use in carrying out any law enforcement, governmental, judicial, or litigation-related function.

96. Douglas has never been charged with or suspected of committing a crime in Hennepin County, has never been involved in any civil, criminal, administrative, or arbitral proceeding in or involving Hennepin County, has never had dealings with Hennepin County Economic Assistance and there was no legitimate reason for Plaintiff to have been the subject of any investigation by Hennepin County.

97. Rather, Hennepin County's obtainment and use of Plaintiff's personal information was for purposes that were purely personal to Hennepin County's personnel.

98. Officers employed by, licensed by, or otherwise accessing through Kanabec County obtained Douglas' Private Data, as reflected in Exhibit A for purposes not permitted by the DPPA one time.

99. Defendant Kanabec County's obtainment and use of Plaintiff's personal information was not for any use in carrying out any law enforcement, governmental, judicial, or litigation-related function.

100. Douglas has never been charged with or suspected of committing a crime in Kanabec County, has never been involved in any civil, criminal, administrative, or arbitral proceeding in or involving Kanabec County, and there was no legitimate reason for Plaintiff to have been the subject of any investigation by Kanabec County.

101. Rather, Kanabec County's obtainment and use of Plaintiff's personal information was for purposes that were purely personal to Kanabec County's personnel.

102. Officers employed by, licensed by, or otherwise accessing through the City of Minnetonka obtained Douglas' Private Data, as reflected in Exhibit A for purposes not permitted by the DPPA three times.

103. Defendant Minnetonka's obtainment and use of Plaintiff's personal information was not for any use in carrying out any law enforcement, governmental, judicial, or litigation-related function.

104. Douglas has never been charged with or suspected of committing a crime in the City of Minnetonka, has never been involved in any civil, criminal, administrative, or arbitral proceeding in or involving the City of Minnetonka, and there was no legitimate reason for Plaintiff to have been the subject of any investigation by the City of Minnetonka.

105. Rather, the City of Minnetonka's obtainment and use of Plaintiff's personal information was for purposes that were purely personal to the City of Minnetonka's personnel.

106. Officers employed by, licensed by, or otherwise accessing through the City of Mound obtained Douglas' Private Data, as reflected in Exhibit A for purposes not permitted by the DPPA one time.

107. Defendant Mound's obtainment and use of Plaintiff's personal information was not for any use in carrying out any law enforcement, governmental, judicial, or litigation-related function.

108. Dougals has never been charged with or suspected of committing a crime in the City of Mound, has never been involved in any civil, criminal, administrative, or arbitral proceeding in or involving the City of Mound, and there was no legitimate reason for Plaintiff to have been the subject of any investigation by the City of Mound.

109. Rather, the City of Mound's obtainment and use of Plaintiff's personal information was for purposes that were purely personal to the City of Mound's personnel.

110. Officers employed by, licensed by, or otherwise accessing through the City of Rosemount obtained Douglas' Private Data, as reflected in Exhibit A for purposes not permitted by the DPPA two times.

111. Defendant Rosemount's obtainment and use of Plaintiff's personal information was not for any use in carrying out any law enforcement, governmental, judicial, or litigation-related function.

112. Douglas has never been charged with or suspected of committing a crime in the City of Rosemount, has never been involved in any civil, criminal, administrative, or arbitral proceeding in or involving the City of Rosemount, and there was no legitimate reason for Plaintiff to have been the subject of any investigation by the City of Rosemount.

113. Rather, the City of Rosemount's obtainment and use of Plaintiff's personal information was for purposes that were purely personal to the City of Rosemount's personnel.

114. Officers or personnel employed by, licensed by, or otherwise accessing through St. Louis County obtained Douglas' Private Data, as reflected in Exhibit A for purposes not permitted by the DPPA two times.

115. Defendant St. Louis County's obtainment and use of Plaintiff's personal information was not for any use in carrying out any law enforcement, governmental, judicial, or litigation-related function.

116. Douglas has never been charged with or suspected of committing a crime in St. Louis County, has never been involved in any civil, criminal, administrative, or arbitral proceeding in or involving St. Louis County, and there was no legitimate reason for Plaintiff to have been the subject of any investigation by St. Louis County.

117. Rather, St. Louis County's obtainment and use of Plaintiff's personal information was for purposes that were purely personal to St. Louis County's personnel.

118. Officers employed by, licensed by, or otherwise accessing through the City of St. Paul obtained Douglas' Private Data, as reflected in Exhibit A for purposes not permitted by the DPPA eight times.

119. Defendant St. Paul's obtainment and use of Plaintiff's personal information was not for any use in carrying out any law enforcement, governmental, judicial, or litigation-related function.

120. Douglas has never been charged with or suspected of committing a crime in the City of St. Paul, has never been involved in any civil, criminal, administrative, or arbitral proceeding in or involving the City of St. Paul, and there was no legitimate reason for Plaintiff to have been the subject of any investigation by the City of St. Paul.

121. Rather, the City of St. Paul's obtainment and use of Plaintiff's personal information was for purposes that were purely personal to the City of St. Paul's personnel.

122. Officers employed by, licensed by, or otherwise accessing through the Metropolitan Airport Commission obtained Douglas' Private Data, as reflected in Exhibit A for purposes not permitted by the DPPA one time.

123. Defendant Metropolitan Airport Commission's obtainment and use of Plaintiff's personal information was not for any use in carrying out any law enforcement, governmental, judicial, or litigation-related function.

124. Douglas has never been charged with or suspected of committing a crime on the premises of the Metropolitan Airport Commission, has never been involved in any civil, criminal, administrative, or arbitral proceeding in or involving the Metropolitan Airport Commission, and there was no legitimate reason for Plaintiff to have been the subject of any investigation by the Metropolitan Airport Commission.

125. Rather, the Metropolitan Airport Commission's obtainment and use of Plaintiff's personal information was for purposes that were purely personal to the Minneapolis Airport Commission's personnel.

126. Personnel employed by, licensed by, or otherwise accessing through Hire Right obtained Douglas' Private Data, as reflected in Exhibit A for purposes not permitted by the DPPA five times.

127. Defendant Hire Right's obtainment and use of Plaintiff's personal information was not for any use in carrying out any law enforcement, governmental, judicial, or litigation-related function.

128. Plaintiff has never been involved in any civil, criminal, administrative, or arbitral proceeding in or involving Hire Right, and there was no legitimate reason for Plaintiff to have been the subject of any investigation by Hire Right.

129. Rather, Hire Right's obtainment and use of Plaintiff's personal information was for purposes that were purely personal to Hire Right's personnel.

130. Officers employed by, licensed by, or otherwise accessing through Beltrami County obtained Nancy's Private Data, as reflected in Exhibit B for purposes not permitted by the DPPA one time.

131. Defendant Beltrami County's obtainment and use of Plaintiff's personal information was not for any use in carrying out any law enforcement, governmental, judicial, or litigation-related function.

132. Nancy has never been charged with or suspected of committing a crime in Beltrami County, has never been involved in any civil, criminal, administrative, or arbitral proceeding in or involving Beltrami County, and there was no legitimate reason for Plaintiff to have been the subject of any investigation by Beltrami County.

133. Rather, Beltrami County's obtainment and use of Plaintiff's personal information was for purposes that were purely personal to Beltrami County's personnel.

134. Officers employed by, licensed by, or otherwise accessing through Carlton County obtained Nancy's Private Data, as reflected in Exhibit B for purposes not permitted by the DPPA one time.

135. Defendant Carlton County's obtainment and use of Plaintiff's personal information was not for any use in carrying out any law enforcement, governmental, judicial, or litigation-related function.

136. Nancy has never been charged with or suspected of committing a crime in Carlton County, has never been involved in any civil, criminal, administrative, or arbitral proceeding in or involving Carlton County, and there was no legitimate reason for Plaintiff to have been the subject of any investigation by Carlton County.

137. Rather, Carlton County's obtainment and use of Plaintiff's personal information was for purposes that were purely personal to Carlton County's personnel.

138. Officers employed by, licensed by, or otherwise accessing through the City of Eden Prairie obtained Nancy's Private Data, as reflected in Exhibit B for purposes not permitted by the DPPA two times.

139. Defendant Eden Prairie's obtainment and use of Plaintiff's personal information was not for any use in carrying out any law enforcement, governmental, judicial, or litigation-related function.

140. Nancy has never been charged with or suspected of committing a crime in the City of Eden Prairie, has never been involved in any civil, criminal, administrative, or arbitral proceeding in or involving the City of Eden Prairie, and there was no legitimate reason for Plaintiff to have been the subject of any investigation by the City of Eden Prairie.

141. Rather, the City of Eden Prairie's obtainment and use of Plaintiff's personal information was for purposes that were purely personal to the City of Eden Prairie's personnel.

142. Officers employed by, licensed by, or otherwise accessing through Kanabec County obtained Nancy's Private Data, as reflected in Exhibit B for purposes not permitted by the DPPA two times.

143. Defendant Kanabec County's obtainment and use of Plaintiff's personal information was not for any use in carrying out any law enforcement, governmental, judicial, or litigation-related function.

144. Nancy has never been charged with or suspected of committing a crime in Kanabec County, has never been involved in any civil, criminal, administrative, or arbitral proceeding in or involving Kanabec County, and there was no legitimate reason for Plaintiff to have been the subject of any investigation by Kanabec County.

145. Rather, Kanabec County's obtainment and use of Plaintiff's personal information was for purposes that were purely personal to Kanabec County's personnel.

146. Officers employed by, licensed by, or otherwise accessing through the City of St. Paul obtained Nancy's Private Data, as reflected in Exhibit B for purposes not permitted by the DPPA one time.

147. Defendant St. Paul's obtainment and use of Plaintiff's personal information was not for any use in carrying out any law enforcement, governmental, judicial, or litigation-related function.

148. Nancy has never been charged with or suspected of committing a crime in the City of St. Paul, has never been involved in any civil, criminal, administrative, or arbitral proceeding in or involving the City of St. Paul, and there was no legitimate reason for Plaintiff to have been the subject of any investigation by the City of St. Paul.

149. Rather, the City of St. Paul's obtainment and use of Plaintiff's personal information was for purposes that were purely personal to the City of St. Paul's personnel.

150. Officers or personnel employed by the Entity Defendants, along with those Individual Defendants currently identified as John and Jane Does, obtained or used Douglas' Private Data approximately eighty-three (83) times.

151. Officers employed by the Entity Defendants, along with those Individual Defendants currently identified as John and Jane Does, obtained or used Nancy's Private Data approximately twelve (12) times.

152. Each of the above accesses was committed knowingly; each of the above accesses was for a reason not permitted under the DPPA, meaning that the Defendants had no law-enforcement reason for accessing the information.

153. Defendants accessed the information for personal reasons completely unrelated to their position as law-enforcement officers, public employees, or in their job functions.

154. Individual Defendants viewed Plaintiffs' Private Data from their State-issued driver's license including their home address, color photographs or images, dates of birth, eye colors, heights, weights, medical information, driver identification numbers, and upon information and belief, social security information.

155. Curiosity about Plaintiffs or other personal reasons are not purposes permitted for obtaining information under the DPPA.

156. The Individual Defendants mentioned above who obtained this information did so using Plaintiffs' names, not pursuant to a license plate look-up, and there is seldom any law- enforcement function that would permit accessing Plaintiffs' private information by name; Plaintiffs were not involved in any criminal activity nor suspected of any such activity; they had not committed any act that would entitle Entity Defendants and Individual Defendants to obtain their information under any of the permissible exceptions; to the extent any such permissible reason could exist, Plaintiffs have

eliminated permissible obtainments from the obtainments here complained of; and no Defendant has proposed a valid, credible reason for obtaining Plaintiffs' information.

157. Under the direction of the Commissioner Defendants, DPS, and DPS Does, knowingly created the DVS Database that includes Plaintiffs' Private Data and the system for law-enforcement personnel to obtain to that information.

158. DPS and DPS Does, under the direction of the Commissioner Defendants, knowingly maintained and updated the DVS Database that included Plaintiffs' Private Data.

159. DPS Commissioners and DPS Does authored the Minnesota Driver's License Application, which states, "your personal information may be *disclosed* as authorized by United States Code, title 18, section 2721." (emphasis added).

160. DPS Commissioners and DPS Does made the decisions for establishing, ordering the structure of, and determining the persons, agencies and individuals to whom they would disclose the database.

161. The disclosure of information was made by providing a user account and a password without reasonably requiring or ensuring that accesses would be limited to those for a purpose permitted under the DPPA.

162. This form of disclosure was and is used not only for law-enforcement personnel but other recipients who have access to the database, including non-government employees, who comprise about half of the persons who have been granted access to this database.

163. DPS Does and Commissioner Defendants failed to use reasonable care in so disclosing the information in the database.

164. DPS Does and Commissioner Defendants made no reasonable effort nor directed any subordinate to make any reasonable effort to require that the specified purpose of the disclosure was legitimate and would be adhered to by the person to whom the data was disclosed.

165. DPS Does and Commissioner Defendants failed to reasonably ascertain or ensure that the persons to whom it was disclosed would use it permissibly.

166. DPS Does and Commissioner Defendants had at the least constructive knowledge of the widespread abuse of the database by officers illegally accessing it for personal reasons not permitted by the DPPA, and had they not delegated their duties to others would have known of the actual misuse and would have presumably fulfilled their statutory duties and prevented the illegal accesses including those that have adversely affected Plaintiffs.

167. DPS Does and Commissioner Defendants knowingly disclosed Plaintiffs' data without requiring that the concomitant obtainment was for a permissible purpose; they disclosed it without taking any effective steps to insure adherence by the individuals—whether private or public sector—obtaining it were or would do so for a permissible purpose.

168. Knowledge of the illegal obtainment of Plaintiffs' information by numerous individuals should be imputed to the DPS Does and Commissioner Defendants based in

part on their delegation to others of their duty to disclose Private Data for only permissible purposes.

169. DPS Does and Commissioner Defendants failed to ascertain or ensure specifically that law-enforcement personnel would use it permissibly, that is, for a law enforcement function.

170. DPS Does and Commissioner Defendants failed to ascertain or ensure that the persons to whom it was disclosed would use it exclusively for a law-enforcement function.

171. DPS Does and Commissioner Defendants failed to provide adequate training in the permissible uses of the database.

172. DPS Does and Commissioner Defendants, under 18 U.S.C. § 2724(a), knowingly disclosed Plaintiffs' personal information for a purpose not permitted by the DPPA.

173. DPS Does and Commissioner Defendants gave Individual Defendants access to the database for purposes of their intended misuse of the database.

174. Disclosure of this database is a matter known to and participated in and directed by the DPS Does and Commissioner Defendants.

175. The DPS Does and Commissioner Defendants had a duty to ascertain the recipients' purpose for his/her obtainment or use of the private data.

176. The DPS Does and Commissioner Defendants, at times, delegated the duty to ascertain the recipients' purpose to other individuals.

177. To the extent the DPS Does and Commissioner Defendants delegated any part of their duties, they are still responsible for disclosure, and the persons, to whom they may have delegated, if any, are not known to Plaintiffs and cannot be known by Plaintiffs.

178. DPS Does and Commissioner Defendants failed to monitor the database through regular, random, target, or user audits to assure themselves that the ongoing disclosures were for permissible purposes in 2003.

179. DPS Does and Commissioner Defendants failed to monitor the database through regular, random, target, or user audits to assure themselves that the ongoing disclosures were for permissible purposes in 2004.

180. DPS Does and Commissioner Defendants failed to monitor the database through regular, random, target, or user audits to assure themselves that the ongoing disclosures were for permissible purposes in 2005.

181. DPS Does and Commissioner Defendants failed to monitor the database through regular, random, target, or user audits to assure themselves that the ongoing disclosures were for permissible purposes in 2006.

182. DPS Does and Commissioner Defendants failed to monitor the database through regular, random, target, or user audits to assure themselves that the ongoing disclosures were for permissible purposes in 2007.

183. DPS Does and Commissioner Defendants failed to monitor the database through regular, random, target, or user audits to assure themselves that the ongoing disclosures were for permissible purposes in 2008.

184. DPS Does and Commissioner Defendants failed to monitor the database through regular, random, target, or user audits to assure themselves that the ongoing disclosures were for permissible purposes in 2009.

185. DPS Does and Commissioner Defendants failed to monitor the database through regular, random, target, or user audits to assure themselves that the ongoing disclosures were for permissible purposes in 2010.

186. DPS Does and Commissioner Defendants failed to monitor the database through regular, random, target, or user audits to assure themselves that the ongoing disclosures were for permissible purposes in 2011.

187. DPS Does and Commissioner Defendants failed to monitor the database through regular, random, target, or user audits to assure themselves that the ongoing disclosures were for permissible purposes in 2012.

188. DPS and DPS Does, under the direction of Commissioner Defendants, had the ability to determine that drivers' license information, including Plaintiffs' Private Data, was being accessed on multiple occasions, by multiple law-enforcement personnel from multiple law-enforcement agencies.

189. DPS and DPS Does, under the direction of the Commissioner Defendants, had the ability to prevent unauthorized access to the DVS Database, including unauthorized access to Plaintiffs' Private Data.

190. DPS and DPS Does, under the direction of the Commissioner Defendants, failed to prevent unauthorized access to the DVS Database, including access to Plaintiffs' Private Data.

191. The Commissioner Defendants and DPS Does knowingly authorized, directed, ratified, approved, acquiesced in, committed or participated in the disclosure of Plaintiffs' Private Data.

192. The policy of the State of Minnesota is to uphold the provisions of the law, both state and federal, and to protect and safeguard the privacy rights of the State's citizens and inhabitants, including its drivers' privacy rights, and including those rights as are required to be protected by federal law.

193. In particular, it is the policy of the State of Minnesota, as outlined in Minn. Stat. § 171.12, subd. 7, to comply with the provisions and requirements of the DPPA.

194. This policy is also set forth in the driver's license application and set forth in statutory language with proper citation to that federal statute.

195. Defendant Commissioners and DPS Does knowingly disclosed Plaintiffs' and others' Private Data and violated state policy by devising and implementing a database, such as the DVS Database, that failed abysmally to uphold the privacy rights of Plaintiffs and others similarly situated as protected by the DPPA.

196. This failure exposed their information to impermissible and knowing accesses by various persons, including the Defendants in this lawsuit.

197. These acts and failures to act by Defendant Commissioners and DPS Does constitute knowing disclosures of Plaintiffs' information within the meaning of the DPPA.

198. Defendant Commissioners and DPS Does knowingly devised and implemented a database and a method for using and misusing that database that both

permitted and encouraged, through the nature and monitoring of the system, accesses by law-enforcement personnel, state employees, and others that failed to comply with state policy of protecting privacy rights and complying with the DPPA.

199. The system knowingly devised and implemented by Commissioner Defendants and DPS Does failed to set rules protecting Plaintiffs' privacy rights.

200. This system permitted, and on information and belief still permits, the accessing of the database from personal computers.

201. This system allowed individuals to give out their personal passwords to others.

202. This system permitted, and on information and belief may still permit, the accessing of the system by persons without any accountability or even in some instances without the ability to trace the person who made the access.

203. From 2003 through 2010, this system did not require reasonably adequate training on the use of the DVS database of sworn-law enforcement officers.

204. From 2011 through today, this system still does not require reasonably adequate training on the use of the DVS database of sworn law-enforcement officers.

205. Accordingly, the effective monitoring of the system is difficult if not impossible under the system as devised and implemented by Commissioner Defendants and DPS Does.

206. Commissioner Defendants and DPS Does have deliberately emphasized and favored the convenience of the system by users at the expense of protecting the privacy rights of the persons whose information is in the database.

207. This deliberate emphasis and preference for convenience to the system users over the privacy rights of the drivers was known to the Commissioner Defendants and the DPS Does, and was purposeful.

208. In failing to properly implement, maintain, and monitor the DVS Database, Commissioner Defendants failed to follow Minnesota state policy.

209. Many viable methods were and are available to prevent this illegal accessing of private information.

210. Upon information and belief, the Commissioners and DPS Does actually knew that law-enforcement officers were accessing the databases for purposes not permitted under the DPPA.

211. Upon information and belief, the Commissioners and DPS Does actually knew that law-enforcement officers were viewing Plaintiffs' Private Data without a legitimate and purpose permitted by the DPPA.

212. Upon information and belief, the Commissioners and DPS Does acquiesced, facilitated, approved, or simply ignored the improper conduct by governmental personnel.

213. Even if the Commissioners and DPS Does had no actual knowledge of the impermissible uses of the databases they oversaw, upon information and belief, they were reckless in their supervision of their subordinates who did operate the database.

214. Upon information and belief, the Commissioners and DPS Does were negligent in supervising their subordinates who operated the databases.

215. The information contained in the DPS database is far greater and contains more private personal information than is customarily known to non-law enforcement personnel.

216. The information contained in the DPS database includes the social security numbers of the drivers, including Plaintiffs' social security numbers.

217. The information contained in the DPS database includes drivers' health information.

218. These accesses are committed surreptitiously, and without the knowledge of the victims, including Plaintiffs, which knowledge is kept hidden and concealed from the victims, including Plaintiffs.

219. There has not been a single instance of which Plaintiffs are aware involving them or anyone else where an officer has informed them that he or she has accessed their information.

220. Law-enforcement officers have gone to great lengths to avoid letting Plaintiffs know they have accessed their personal private information.

221. The surreptitious, concealed, and hidden accesses are kept secret from the general public and from the victims, including Plaintiffs.

222. Commissioner Defendants and DPS Does allowed multiple breaches of the security of Plaintiffs' Private Data in violation of Minn. Stat. 13.055.

223. Commissioner Defendants and DPS Does failed to disclose to Plaintiffs this breach of the security of the data in violation of Minn. Stat. 13.055.

224. Obtaining the DVS Database without a permissible reason is a breach of confidentiality.

225. Plaintiffs contacted DPS to inquire whether law-enforcement officers had been viewing their private information.

226. The DPS website states that the public is entitled to information except that which is classified:

> [T]he law states that all the data DPS or a governmental entity has are public (can be seen by anybody) unless there is a state or federal law that classified the data as not public. You have the right to look at all public data that DPS keeps.
>
> (*See* Minnesota Department of Public Safety: Public Access to Government Data," attached to this Complaint as Exhibit C).

227. The DPS website also informs the public that anyone can request information in any way, by phone, in person, mail, or email; that specific data can be requested, or "entire records, files or data bases" or all public data that DPS keeps." It instructs the person requesting the information that "you don't have to tell us who you are or explain why you are asking for the data." *Id*.

228. But despite its stated policy, before August 2011, the actual practice of DPS was to withhold, deny and mislead the public to prevent access to this information. (*See* Affidavit of Dan Prozinski, attached to this Complaint as Exhibit D; August 23, 2011 email from Joseph Newton to A. Geraghty, attached to this Complaint as Exhibit E; and the Second Amended Complaint to *Kampschroer v. Anoka Cty., et. al*, 13-2512 SRN/TNL, at ¶¶ 410 – 426).

229. DPS practice in this regard amounted to concealment of the illegality, by misleading the public on those occasions when they became suspicions about the invasion of their private data.

230. These invasions or illegal accesses of their Private Data were by their very nature actively concealed, since those making the accesses concealed them from their supervisors and from Plaintiffs; at no time did anyone approach Plaintiffs and advise them that he or she had accessed their Private Data.

231. In 2013, Plaintiffs requested an audit from Kim Jacobson at DPS.

232. The Minnesota Department of Motor Vehicles is a division of DPS.

233. On October 1, 2013, Jacobson provided the results of the audit to Douglas.

234. On November 27, 2013, Jacobson provided the results of the audit to Nancy.

235. The audit requests and the results furnished, were for name look-ups only and specifically did not include any license plate or driver's license number look-ups.

236. Douglas was sickened to learn from DPS that it had determined that officers and personnel from approximately several different departments and agencies had reviewed, and impermissibly obtained or used, his Private Data approximately 83 times since 2003. *See* Exhibit A.

237. Nancy was similarily sickened to learn from DPS that it had determined that officers and personnel from approximately several different departments and agencies had reviewed, and impermissibly obtained or used, her Private Data approximately 12 times since 2004. *See* Exhibit B.

238. Before requesting the audit report, Plaintiffs had no knowledge that their Private Data had been obtained through the DVS Database.

239. Plaintiffs were not under any criminal investigation; they had committed no crimes; they were not seeking the assistance of law-enforcement; they were not a witness to any crime, nor were they involved with anyone in a criminal investigation; they were not of any legitimate interest to law-enforcement other than for personal reasons, such as curiosity attraction.

240. Douglas has not been stopped for a traffic violation since approximately 1995.

241. Nancy has never been stopped for a traffic violation in the State of Minnesota.

242. There is no possible law-enforcement function that would have made invading Plaintiff' privacy permissible under the DPPA.

243. Plaintiffs believe that even more unauthorized accesses and viewings will occur in the future if the policies of Entity Defendants and other police departments and law-enforcement agencies similarly situated are not changed to bring the actual custom and practice of these Entity Defendants and others similarly situated into compliance with their own written rules, with the rules of the Department of Public Safety, and with federal law, including the DPPA.

244. Included in the audit is the listing of various law-enforcement departments associated with the Defendant Entities that obtained Plaintiffs' Private Data.

245. Individual Defendants' identities (John and Jane Does) are not presently known, and purportedly cannot be revealed pursuant to the Minnesota Government Data Practices Act. Plaintiffs anticipate that these yet-to-be-named Individual Defendants will become known through discovery.

246. Supervisor Defendants are not presently known. Plaintiffs anticipate that the yet-to-be-named Supervisor Defendants who should have monitored, prevented and stopped the unauthorized accesses to Plaintiffs' information will become known through discovery.

247. The remaining Entity Defendant identities (Entity Does) are not presently known, because not all of the entities identified by the DPS have provided sufficient information to determine if their personnel's access to the database was unauthorized. Plaintiffs anticipate that these yet-to-be-named Entity Defendants will become known through discovery.

248. Defendant Commissioners released and disclosed this information without training or with wholly inadequate training for the individuals with access to the DVS database.

249. Defendant Commissioners released and disclosed Plaintiffs' Private Data to individuals without ascertaining whether it was obtained for a purpose permitted under the DPPA, but instead relied on the status of the person obtaining it, assuming that because of the person's status their obtainment of the information was for a purpose permitted by the DPPA.

250. Whatever training, monitoring, or inquiry into the officers' usage of the information systems has been adopted is woefully inadequate to ensure that access is used properly and lawfully.

251. On information and belief, despite this training, Defendant Entities and Defendant Supervisors, allowed their employees, including but not limited to Individual Defendants, to view Plaintiffs' Private Data for unlawful purposes.

252. On information and belief, Defendant Entities, Defendant Supervisors, and Commissioner Defendants permitted, condoned, or acquiesced in this illegal access to Plaintiffs' private information, and knew or should have known that it was occurring.

253. On information and belief, this illegal access occurs with regularity not only of Plaintiffs' private information, but of other Minnesota drivers' private information.

254. Defendant Entities, Defendant Supervisors, Defendant Commissioners and DPS Does have lax policies or lax enforcement of these policies that allow for these intrusions.

255. Defendant Entities, Defendant Supervisors, Defendant Commissioners and DPS Does either have no viable method of or have an inadequate method of ascertaining and controlling the illegal access to individuals' private information by their officers.

256. The Driver's License application assures Minnesota drivers their information will be safeguarded and kept private, "DPS releases this information to local, state, and federal government agencies only as authorized or required by state and federal law."

257. Plaintiffs submitted their Private Data to DPS, including their social security numbers, because of the promise of confidentiality made by DPS.

258. Plaintiffs relied on this promise of confidentiality when they provided their Private Data to DPS to obtain a driver's license.

259. The failure of Defendant Entities and Defendant Supervisors to keep this information private is a flagrant breach of a promise of confidentiality.

260. Defendant Entities, Defendant Supervisors, Commissioner Defendants, and DPS Does either have no viable method of or have an inadequate method of ascertaining and controlling the illegal access to individuals' private information by their officers.

261. The extent of this illegal access is widespread and pervasive throughout departments, and is a custom and practice.

262. The widespread practice is demonstrated by the systematic tolerance of illegal accesses.

263. Further evidence of the custom and practice can be found in actual statements made by current officers, one of whom was quoted in a magazine article about the illegal access into previous cases involving this same breach of privacy as saying that "every single cop in the state has done this. Chiefs on down."

264. Further evidence is based on actual statements made by former officers, one of whom was quoted in a magazine article about illegal accesses of other individuals as saying that "[y]ou used to look up people without a second thought. You'd look up old friends from high school or just someone you used to know."

265. Each individual with access to the DPS Database has a password allowing that individual access to the DPS Database.

266. Personnel can access the DPS Databases from any computer with internet access.

267. Personnel occasionally gave other individuals their passwords, contrary to requirements.

268. The system for accessing accountability and responsibility was and is prone to error and fails to reasonably protect drivers' private information.

269. When Defendant personnel viewed Plaintiffs' private information, they did not do so to carry out official police functions.

270. Plaintiffs committed no crimes or transgressions that would explain or legitimize the unauthorized access of their Private Data.

271. The Individual Defendants obtained Plaintiffs' personal information without probable cause or reasonable suspicion to believe that Plaintiffs had engaged in any criminal activity or any activity even remotely related to criminal activity.

272. Plaintiffs never waived the protections of the DPPA.

273. Defendants' actions have violated the United States Constitution, the DPPA, 42 U.S.C. § 1983, and Minnesota State law.

274. The sheer volume of the intrusions into their private life demonstrates that law-enforcement personnel, public employees, and others are unfairly hostile and careless toward Plaintiffs' privacy and safety.

275. As a result of these invasions of privacy, Plaintiffs have suffered and continue to suffer severe emotional distress.

THE COMMISSIONERS HAVE KNOWN ABOUT THESE VIOLATIONS

276. DPS Commissioners Campion and Dohman have been involved with law enforcement for many years.

277. Commissioner Dohman has been a law enforcement officer for thirty years, having formerly served as police chief of the City of Maple Grove from 2001 until her appointment as DPS Commissioner in March 2011.

278. Before becoming Chief of Police of the Maple Grove Police Department she was an investigator, patrol officer, sergeant and captain of the Maple Grove Police Department; and prior to that time, she was a patrol officer of the City of Glencoe and of the City of Marshall, Minnesota.

279. Dohman also served as president of the Minnesota Chiefs of Police Association.

280. Upon information and belief, the misuse of private information is the main complaint of most police chiefs and human resources personnel.

281. Former Commissioner Michael Campion served from July 2004 until March 2011. Prior to his appointment as DPS Commissioner he was supervisor of the BCA, which also maintains a driver's license database.

282. Prior to that position, Campion was a special agent at the BCA.

283. It was during his tenure that the DPS database was largely developed in its current format.

284. On information and belief, misuse of the DPS database has been well-known to Commissioner Defendants. At a Legislative Audit Subcommittee hearing in February, 2013 at which Commissioner Dohman testified, the testimony of the Legislative Auditor revealed that at least 50% of law enforcement officers are misusing the DPS database by obtaining, disclosing, and/or using the driver license personal information for an impermissible purpose.

285. On information and belief, Commissioner Defendants knew this, and knowingly disclosed the information in part by (a) failing to safeguard and monitor the database despite knowing of its rampant misuse, (b) willfully refusing to correct the misuses, or (c) both failing to monitor and refusing to correct the abuse and misuse of the system.

286. Experts in the field of police training report that the primary complaint of many police departments is that law enforcement personnel misuse private information. This is an established, well-known, and pervasive problem with law enforcement that Commissioner Defendants are unwilling to properly address.

THE COMMISSIONER DEFENDANTS AND DPS DOES REASONABLY COULD HAVE DONE SIGNIFICANTLY MORE TO PROTECT PLAINTIFFS' PRIVACY.

287. On information and belief, the only changes and improvements to the DPS system to increase the protection of privacy, especially from law enforcement, have occurred only after litigation involving DPS, specifically the lawsuit titled Anne Marie Rasmusson v. City of Bloomington, No. 12-CV-00632 (SRN/JSM). In that case Plaintiff

sued, among others, the Commissioners of the DPS and was able to obtain through settlement significant changed to the DVS database, including numerous protections such as different types of periodic audits. On information and belief, the 19,000 improper accesses of former Department of Natural Resources Captain John Hunt were discovered in part due to those changes. The vast majority of the restrictions and protections on driver privacy have occurred due to the Rasmusson case and others like it. The Commissioners in Minnesota remain highly resistant to improving the DPS database, instead looking to the individual officers and local governments to institute changes, which is a far less effective method of instituting changes and will result in piecemeal and inadequate changes in protections at best.

288. On information and belief, states other than Minnesota have far greater restrictions and protections in place to protect the data on their drivers' license databases from being obtained, disclosed or used for a reason not permitted by the DPPA.

289. For instance, on further information and belief, North Dakota requires a daily report of anyone who obtains driver photos and its system generates weekly reports listing all individuals with accesses of over 25 images a day. These reports are sent to the North Dakota Attorney General to make inquiries as to whether the information was obtained for a job-related reason. North Dakota also requires the users of the database to declare the reason why they were looking at the record. North Dakota also requires its users to take a certification test before being given access to the database.

290. Also on information and belief, the State of California's DMV cooperates with its law-enforcement agencies and California's Department of Justice to ensure

access to its drivers' license information is limited to agencies that satisfy specific requirements before they are issued a confidential requester code that permits access to law-enforcement information only. Each law-enforcement agency is responsible for limiting access to necessary personnel. California also periodically reviews law-enforcement applications to ensure the agency and person requesting the information is still entitled to obtain the information. During a recent audit, California's DMV reviewed questionable agencies and even reclassified some to prevent them from having further access to the database.

291. On further information and belief, the California DMV has a dedicated law-enforcement unit to analyze data inquiries. Each data request is logged and technicians are trained to look for developing patterns in the requester's history. The California DMV also conducts periodic historical reviews of a specific agency's requests to determine if the accesses were authorized. The California DMV may also require a law-enforcement entity to supply an explanation of events, describe their protocols for accessing DMV information, what policies or access requirements were violated, what corrective or administrative steps are being taken to admonish the officer, and what steps the agency is taking to avoid future occurrences. All users annually complete an information security form. Finally, the California DMV is very restrictive on the types of information it releases.

292. On information and belief, DPS Commissioners, DPS and Defendants Entities knew or should have known of the policies and practices of other States, but did not a the time that Plaintiffs' drivers' license information was being impermissibly

obtained, require any of the protections and safeguards to the Minnesota DPS Databases utilized by other states.

293. Given that other states do and did have safeguards and protections in place to protect their drivers' private information from impermissible accessing, use, and disclosure, DPS Commissioners, DPS and Defendants Entities reasonably should have implemented such safeguards and protections for Minnesota drivers, including Plaintiffs.

294. The implementation of some or all of these safeguards and protections by Defendants would have prevented many of the impermissible obtainment, uses, and disclosures of Plaintiffs' private data.

COUNT I: VIOLATION OF THE DPPA, 18 U.S.C. § 2721, *et seq.*

(Against all Defendants)

295. Plaintiffs reaffirm and reallege the allegations in Paragraphs 1 through 294

296. Plaintiffs provided personal information to the DPS including their address, color photograph, date of birth, weight, height, eye color, social security numbers and medical information for the purpose of acquiring and utilizing a State of Minnesota driver's license.

297. The DPS Database also maintained Plaintiffs' driving record.

298. Plaintiffs did not provide their consent for any of Defendant Individuals to obtain, disclose or use, or for any of Defendant Entities or Defendant Supervisors to disclose or to allow Defendant Individuals to obtain, disclose or use, their private information for anything but official law-enforcement business.

299. Knowingly obtaining, disclosing or using Private Data for a purpose not permitted by the DPPA is a violation of the DPPA. The statute provides for criminal fines and civil penalties. 18 U.S.C. §§ 2723, 2724.

300. The DPPA provides redress for violations of a person's protected interest in the privacy of their motor vehicle records and the identifying information therein.

301. Minnesota law is to enforce and follow the DPPA and to hold all information obtained pursuant to an application for a driver's license confidential and private; even prior to the passage of the DPPA in 1994 Minnesota law pledged to hold all this information private and confidential, and on one's driver's license application these promises of confidentiality are all made; Defendants' actions in accessing this information is a flagrant breach of that pledge of confidentiality.

302. Each of the Defendants invaded Plaintiffs' legally protected interest under the DPPA.

303. According to the Department of Vehicle Services, the Individual Defendants knowingly obtained, disclosed or used Plaintiffs' personal information, from a motor vehicle record, for a purpose not permitted under the DPPA. 18 U.S.C. § 2724(a).

304. None of the Individual Defendants' activities fell within the DPPA's permitted exceptions for procurement of Plaintiffs' private information.

305. By the actions described above, each Defendant Individual was acting within the scope of his or her employment when he or she obtained, disclosed or used

Plaintiffs' personal information from the DPS Databases for a purpose not permitted by the DPPA.

306. Individual Defendants knew that their actions related to Plaintiffs' Private Data were in violation of the DPPA.

307. Defendant Entities and Defendant Supervisors knowingly authorized, directed, ratified, approved, acquiesced in, committed or participated in obtaining, disclosing or using of Plaintiffs' private personal information by Individual Defendants.

308. Defendant Commissioners, Defendant Entities and Defendant Supervisors' actions constitute a knowing disclosure of the personal information of Plaintiffs under the DPPA.

309. Individual Defendants knowingly used Defendant Entities' computers, passwords and passcodes to obtain Plaintiffs' private information.

310. Plaintiffs' private information was obtained by each Individual Defendant for purposes that are not permitted under the DPPA.

311. Defendant Entities are each vicariously liable for the acts of Defendant Individuals.

312. By the actions complained of, Commissioner Defendants, and DPS Does are jointly liable for the acts of Defendant Individuals.

313. Plaintiffs have suffered harm because their private information has been obtained and viewed unlawfully.

314. Plaintiffs suffer and continue to suffer harm by virtue of the increased risk that their protected information is in the possession of Individual Defendants who obtained it without a purpose permitted under the DPPA.

315. This is precisely the harm Congress sought to prevent by enacting the DPPA and its statutory remedies.

316. Individual Defendants, Supervisor Defendants, and Commissioner Defendants each willfully and recklessly disregarded the law, entitling Plaintiffs to punitive damages under the DPPA, see 18 U.S.C. § 2724(b)(2), which is not subject to the pleading requirement of Minnesota state law as set forth in Minn. Stat. § 549.20. Plaintiffs are entitled to actual damages, punitive damages, reasonable attorneys' fees and other litigation costs reasonably incurred, and such other preliminary and equitable relief as the court determines to be appropriate. 18 U.S.C. § 2724(b).

317. In addition, under the DPPA, Plaintiffs are entitled to a baseline liquidated damages award of at least $2,500 for each violation of the DPPA. 18 U.S.C. § 2721(b)(1). Plaintiffs need not prove actual damages to receive said liquidated damages.

COUNT II: VIOLATION OF 42 U.S.C. § 1983

(Against All Individual Defendants Including Jane and John Does except for employees of Hire Right)

318. Plaintiffs reaffirm and reallege the allegations in Paragraphs 1 through 317.

319. The Fourth Amendment to the Constitution of the United States provides for the right of individuals "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."

320. The Fourteenth Amendment provides all individuals in the United States with a substantive due process right of privacy.

321. The Fourth Amendment to the Constitution of the United States establishes a well-settled civil right to be free from an unconstitutional search.

322. At no time did Plaintiffs behave in a manner that would provide any legal justification for the above-described invasion of their privacy.

323. The DPPA establishes that obtaining an individual's Private Data without a legitimate purpose constitutes an illegal search under the meaning of the Fourth Amendment as well as a violation of their substantive due process right to privacy under the Fourteenth Amendment.

324. The DPPA, among other things, such as the plain language of the Constitution, the various court decisions interpreting the Constitution and the traditions of our country establish that an individual has a reasonable expectation of privacy in their driver's license information.

325. Individual Defendants' viewing of Plaintiffs' personal information was unauthorized, unjustified, and excessive, and violates the Fourth and Fourteenth Amendments, the laws of the United States and the laws of the State of Minnesota.

326. By the actions described above, each Individual Defendant, acting under color of state and federal law, violated and deprived Plaintiffs of their Fourth and Fourteenth Amendment Rights.

327. Individual Defendants used the Entity Defendants' computers, passwords and passcodes to obtain Plaintiffs' Private Data.

328. The acts of each Individual Defendant, acting under the color of state and federal law, constituted an invasion or repeated invasions of Plaintiffs' clearly-established privacy rights, guaranteed by the Bill of Rights and the Fourteenth Amendment to the United States Constitution, the laws of the United States, including the DPPA, and the laws of the State of Minnesota.

329. The DPPA protects and codifies an individual right to privacy in a person's Private Data, thereby prohibiting unauthorized accessing of all persons' information, including Plaintiffs' information.

330. Each individual law-enforcement and other government personnel, acting under color of state and federal law, knew that his or her actions violated and deprived Plaintiffs of their clearly established statutory rights under the DPPA.

331. Each Individual Defendant deprived Plaintiffs of their federal statutory rights and civil rights maliciously or by acting with reckless disregard for whether Plaintiffs' rights would be violated by his or her actions.

332. Each Individual Defendant was deliberately indifferent to Plaintiffs' statutory and civil right to be free from illegal searches, invasions of privacy and the unauthorized accessing of their Private Data.

333. As a direct and proximate result of the acts and omissions of the above-named Individual Defendants, Plaintiffs were damaged in an amount yet to determined, but in excess of $75,000.

334. Punitive damages are available against Individual Defendants for their reckless and callous disregard for Plaintiffs' rights and their intentional violations of the

federal law, and are hereby claimed as a matter of federal common law, Smith v. Wade, 461 U.S. 30 (1983), and, as such, are not subject to the pleading requirement for punitive damages set forth in Minn. Stat. § 549.20.

335. Plaintiffs are entitled to recovery of their costs, including reasonable attorney fees, under 42 U.S.C. § 1988.

COUNT III: VIOLATION OF 42 U.S.C. § 1983

(Against Entity Defendants and Supervisor Defendants, including John, Jane and Entity Does, for violation of 42 U.S.C. § 1983, except for Hire Right)

336. Plaintiffs' reaffirm and reallege the allegations in Paragraphs 1 through Paragraph 335.

337. Individual Defendants' numerous accesses of Plaintiffs' private information are not unique, but one example of how frequently such law-enforcement agencies and other governmental entities customarily violate the DPPA by accessing Private Data of persons without having any legitimate or permissible reason for doing so.

338. Persons familiar with police departments and those involved in teaching supervisors how to train and hold accountable their subordinate law-enforcement personnel have been told by those supervisors that the unlawful and impermissible accessing of private information is among the most frequently committed wrongs by police, for which they are seldom if ever held accountable.

339. Improper access of citizens' Private Data by Defendants for their own personal and private uses, obtained by accessing that information through the computerized information storage system kept by the State for official purposes only, is

an official custom or practice well known to Defendant Supervisors and Commissioner Defendants.

340. These customs and practices by Defendant Individuals are at variance with the written rules set down by the Entity Defendants, the DPS, and Commissioner Defendants, but these formal rules are widely and knowingly disregarded.

341. Given Entity Defendants' failure to monitor and enforce their rules, the aforementioned customs and practices are attributable to the municipalities themselves, including the Entity Defendants herein.

342. Defendant Entities and Defendant Supervisors of the law-enforcement personnel and other public employees accessing this information knew or should have known of this and other unlawful, improper, unjustified, and impermissible access to private information by law-enforcement personnel and other public employees.

343. The prevalence of this custom, the lack of monitoring regarding these access practices and the failure to take action to stop or prevent these practices, demonstrate the state of mind of Defendant Supervisors and municipal officials of the Entity Defendants.

344. These customs and practices further demonstrate Defendants' deliberate indifference to the federal statutory and constitutional rights of the citizens and persons, including Plaintiff, whose information has been wrongfully accessed.

345. Defendant Entities are directly liable for the custom and practice of the widespread illegal access of citizens' Private Data.

346. Supervisor Defendants, up to and including the chief police officers and sheriffs employed by each Entity Defendant, are liable in their individual capacity.

347. Defendants' liability is due to their actual and constructive knowledge of this practice.

348. Defendants' liability is also due to their failure to institute any process for monitoring and preventing it.

349. Defendants' liability is also due to their deliberate indifference to the federal rights of those persons, including Plaintiffs, whose information has been and continues to be wrongfully accessed.

350. In addition, Defendant Supervisors of the law-enforcement personnel and other public employees, up to and including the chief police officer in each of Defendant Entities, are liable in their individual capacities for the failure to train, monitor, supervise, and properly discipline the officers who are improperly and unlawfully accessing the Private Data of citizens, including Plaintiffs, without a proper, lawful, permissible, justifiable purpose for doing so.

351. This pattern of failure to train, monitor, supervise, and discipline demonstrates the state of mind of these Defendant Supervisors and a deliberate indifference to the rights of the citizens and others whose information has been so widely accessed, including Plaintiffs.

352. The federal rights of the citizens, including Plaintiffs, whose information was improperly accessed, are held in light regard by many if not most of the Defendant Supervisors and by the Defendant Entities themselves.

353. Defendants' lack of concern evidences their deliberate indifference both to the problem of the unauthorized access and to the impact of the unauthorized access on the federal rights of the citizens, including Plaintiffs, who would often be unaware of that access.

354. It is yet unknown whether a system has been established by the Entity Defendants and Supervisor Defendants to monitor the regular access of the DPS Databases by personnel.

355. It is yet unknown whether any attempt has been made by Entity Defendants and Supervisor Defendants to provide redress and assurance to the persons, including Plaintiffs, whose DVS information has been wrongfully accessed by the Individual Defendants named in this Complaint, or by other personnel in the municipalities named in this Complaint.

356. As a direct and proximate result of the acts and omissions of the above-named Defendant Entities and Defendant Supervisors, Plaintiffs have endured and continue to endure mental suffering, and have been damaged in an amount yet to be determined and of a continuing nature, but in an amount in excess of $75,000.

357. Punitive damages are available against Defendant Supervisors for their reckless and callous disregard for Plaintiffs' rights and their intentional violations of the federal law, and are hereby claimed as a matter of federal common law, Smith v. Wade, 461 U.S. 30 (1983), and, as such, are not subject to the pleading requirements set forth in Minn. Stat. § 549.20.

358. Plaintiffs are entitled to recovery of their costs, including reasonable attorney fees, under 42 U.S.C. § 1988.

COUNT IV: VIOLATION OF 42 U.S.C. § 1983

(Against Commissioner Defendants and DPS Does)

359. Plaintiffs reaffirm and reallege the allegations in Paragraphs 1 through 358.

360. As DPS Commissioners, Campion and Dohman, along DPS Does, were and are responsible for creating, maintaining, and providing access to the database that included Plaintiffs' Private Data.

361. Defendant Commissioners and DPS Does also had the ability to determine if unauthorized access was being made and to prevent such unauthorized access to the database, including of Plaintiffs' Private Data, and have the ongoing duty to prevent such unauthorized accesses.

362. Defendant Commissioners and DPS Does failed to utilize any due care to ensure that the disclosed information was being used only for permissible purposes.

363. Commissioner Defendants and DPS Does failed to prevent unauthorized access to the database, including Plaintiffs' Private Data.

364. The actions of Commissioner Defendants and DPS Does, as alleged, violate the rights of Plaintiffs under the Fourth and Fourteenth Amendments to the United States Constitution and under the DPPA.

365. On information and belief, Commissioner Defendants, and DPS Does created or oversaw the creation and maintenance of a database and system that was supposed to prevent unauthorized access to Private Data.

366. From 2003, Commissioner Defendants and DPS Does allowed unauthorized access of Douglas' Private Data about 83 times.

367. From 2004, Commissioner Defendants and DPS Does allowed unauthorized access of Nancy's Private Data about 12 times.

368. On information and belief, Commissioner Defendants' and DPS Does' efforts have been insufficient to prevent future unauthorized access of Plaintiffs' and other individuals' private, personal information.

369. Commissioner Defendants and DPS Does have sanctioned the constitutional violations by the Individual Defendants through their failure to remedy the policy, custom and practice of officers' and employees' unfettered and unauthorized access to the database.

370. Commissioner Defendants and DPS Does have been negligent in supervising subordinates responsible for implementing a law-enforcement database that prevents unauthorized access to private, personal information.

371. On information and belief, Commissioner Defendants and DPS Does failed to monitor and prevent unauthorized access to private, personal information even though they knew or should have known that such unconstitutional acts were occurring.

372. Commissioner Defendants and DPS Does, acting under the color of state law, were deliberately indifferent to Plaintiffs' constitutionally-recognized and federal statutory rights to be free from illegal searches, invasions of privacy and the unauthorized accessing of their Private Data.

373. Commissioner Defendants and DPS Does failed to implement properly Minnesota's policy to protect the private, personal information of its citizens with drivers' licenses.

374. Commissioner Defendants and DPS Does are jointly liable for the use, disclosure, or access of Plaintiffs' Private Data for each Individual Defendants' access.

375. As a direct and proximate result of the acts and omissions of Commissioner Defendants and DPS Does, Plaintiffs were forced to endure physical and mental suffering, and was thereby damaged in an amount yet to determined, but in an amount in excess of $75,000.

376. Punitive damages are available against Commissioner Defendants and DPS Does for their reckless and callous disregard for Plaintiffs'' rights and their intentional violations of the federal law, and are hereby claimed as a matter of federal common law, Smith v. Wade, 461 U.S. 30 (1983), and, as such, are not subject to the pleading requirements set forth in Minn. Stat. § 549.20.

377. Plaintiffs are entitled to recovery of their costs, including reasonable attorney fees, under 42 U.S.C. § 1988.

COUNT V: COMMON LAW INVASION OF PRIVACY

(Against All Defendants)

378. Plaintiffs reaffirm and reallege the allegations in Paragraphs 1 through 377.

379. By improperly obtaining Plaintiffs' private personal information for impermissible reasons, Defendants intentionally intruded upon the solitude or seclusion of Plaintiffs' private affairs and concerns.

380. Defendants' intrusions would be highly offensive to a reasonable person.

381. Defendants' intrusions caused Plaintiffs to suffer severe emotional distress and physical harm.

382. Defendants' intrusions were intended to cause Plaintiffs to suffer severe emotional distress and physical harm, and was made with either actual or legal malice, or with reckless disregard of her rights and her privacy.

383. Plaintiffs are entitled to tort damages for Defendants' invasion of privacy.

JURY DEMAND

384. Plaintiffs demand a jury trial as to all issues of fact herein properly triable to a jury under any statute or under common law.

WHEREFORE, Douglas Delaney and Nancy Delaney pray for judgment against the Defendants as follows:

1. A money judgment against all Defendants for liquidated, actual and compensatory damages in an amount in excess of seventy five thousand ($75,000) dollars and punitive damages in an amount to be determined by the jury, together with their costs, including reasonable attorney fees, under 42 U.S.C. § 1988, the DPPA, and other applicable laws, and prejudgment interest;

2. Actual damages, punitive damages, attorneys' fees and other litigation costs and such other preliminary and equitable relief as the court determines to be appropriate under 18 U.S.C. § 2724(b);

3. Liquidated damages of at least $2,500 for each violation of the DPPA under 18 U.S.C. § 2721(b)(1);

4. An injunction, permanently enjoining all Defendants from viewing Plaintiffs' private information in violation of the DPPA, unless necessary for law enforcement purposes;

5. An injunction, permanently and prospectively requiring Defendants to establish and implement all effective monitoring and investigative procedures to end this practice, discover and suspend permanently all accessing privileges to the violators; and to provide full disclosure to all potential claimants of the entities and persons who have violated their rights under the DPPA and the Constitution; and,

6. For such other and further relief as this Court deems just and equitable.

SAPIENTIA LAW GROUP PLLC

Dated: February 7, 2014

s/ Kenn H. Fukuda
Jonathan A. Strauss (#0279602)
Lorenz F. Fett (#196769)
Sonia Miller-Van Oort (#278087)
Kenn H. Fukuda (#0389301)
12 South Sixth Street, Suite 1242
Minneapolis, MN 55402
(612) 756-7100, Fax: 612-756-7101
jons@sapientialaw.com
larryf@sapientialaw.com
soniamv@sapientialaw.com
kennf@sapientialaw.com

ATTORNEY FOR PLAINTIFFS DOUGLAS DELANEY AND NANCY DELANEY